COMPUTATIONAL IMMUNOLOGY FOR THE DEFENSE OF DISTRIBUTED LARGE SCALE SYSTEMS

Maureen Stillman
Odyssey Research Associates
301 Dates Drive
Ithaca, NY 14850

Stephanie Forrest
Dept. of Computer Science
University of New Mexico
Albuquerque, NM 87131

A scalable intrusion detection framework is a crucial element in any computer-based large-scale system. This framework is missing from many computing environments. The Automated Systems Security Incident Support Team (ASSIST) of the Defense Information Systems Agency (DISA) tested the vulnerability of 12,000 DoD host computers in the unclassified domain. They found that 1-3% of the systems had exploitable front doors and that 88% could be penetrated by network trust relationships. Even more alarming, only 4% of the penetrations were detected and, of those only 5% reported.

Traditional approaches to intrusion detection are problematic for distributed large-scale information systems because they require the collection and analysis of large amounts of data. More specifically, they lack the ability to scale and they lack good methods and tools to understand and/or process this data at either single or multiple locations. We believe that a fresh approach is needed to build effective intrusion detection systems in large-scale distributed environments, to avoid these problems. Our project extends promising new research in computational immunology to build scalable intrusion detection systems.

A successful intrusion detection system for a large-scale information system environment has the following properties: low impact on the general operating environment, easily proved and evaluated, easily deployed and managed, adaptable to new or upgraded environments and dynamic. An additional requirement is that the system be "lightweight." By lightweight we mean the following: real-time detection of intrusions, low false alarm rates, low performance overhead, and a small and compact system which requires no real-time access to volumes of audit record data. Finally, the solution must work in a heterogeneous, distributed environment.

We are taking an immunology-inspired approach to the problem of intrusion detection and applying it to the CORBA environment in order to achieve the goals stated above. Our approach is related to an ongoing research project which is developing ideas for intrusion detection based on immunology and testing them in networked Unix systems. The validation of the immune-based approach in a large-scale distributed environment is

key to determining its success. We are currently working on the definition and implementation of an IDS system architecture for the CORBA environment to validate these research ideas in computational immunology.

A key feature of the immune-inspired approach is to treat a wide range of computer security problems as instances of a problem solved by immunology---that of distinguishing "self" (the body's own cells and molecules) from "other" (everything else). Under this analogy, "self" represents the stable operating conditions of a computer system, and "other" represents the intrusive (or otherwise anomalous) behavior that we wish to prevent. An important aspect of this endeavor is determining an appropriate definition of "self" that compactly characterizes the normal operation of a system such that it can be distinguished from anomalous operation.

Our approach to system architecture is to create small, autonomous agents running on top of ORBs to detect anomalous patterns that are matched against "self". These small agents will report their findings to a hierarchical set of decision making processes, thus handling the problem of scaling up.

This is a joint effort performed by Odyssey Research Associates and Dr. Stephanie Forrest of the University of New Mexico. This work is funded by DARPA and Rome Laboratory under contract number F30602-97-C-0126.